

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **SOUTHERN DISTRICT OF CALIFORNIA**
10

11 UNITED STATES OF AMERICA,
12
13 Plaintiff,
14 v.
15 YE SANG WANG,
16 Defendant.

Case No. 19-cr-1895-BAS

**ORDER DENYING DEFENDANT'S
MOTION TO SUPPRESS EVIDENCE
(ECF No. 92)**

17 Defendant Ye Sang Wang brings a Motion to Suppress all documents seized from
18 her computer including emails between her and her husband and all evidence obtained as
19 a result of this seizure. (ECF No. 92.) The Government opposes (ECF Nos. 94, 95), and
20 Defendant replies (ECF No. 100). For the reasons stated below, the Court **DENIES**
21 Defendant's Motion.

22 **I. BACKGROUND¹**

23 Defendant worked for the Department of Defense (DoD) as a logistics specialist for
24 the Navy. She was responsible for purchasing military equipment for Special
25 Reconnaissance Team I (SRT-I). As such she had a classified security clearance.
26

27 ¹ The summary below is taken from both Defendant's Motion as well as the
28 Government's Response. Unless otherwise indicated, there appears to be no disagreement
between the parties as to the underlying facts.

1 Defendant and her husband, Shaohua Wang, were both naturalized U.S. citizens, originally
2 from the People's Republic of China (PRC).

3 On April 3, 2017, an SRT-I member informed the Naval Criminal Investigative
4 Service (NCIS) that Defendant had attempted to gain a top secret security clearance without
5 the need for one and had travelled to the PRC. NCIS investigated, but subsequently closed
6 the investigation. NCIS did not access Defendant's emails or computer at that time.

7 On March 6, 2018, an SRT-I Special Security Officer contacted a
8 Counterintelligence Support Officer (CISO)—again noting Defendant's repeated inquiries
9 into obtaining a top security clearance. Additionally, the Officer expressed concerns about
10 Defendant compiling a list of future Naval Special Warfare (NSW) Command deployment
11 personnel records, including names and addresses. The CISO accessed and reviewed
12 Defendant's military email account and computer on March 8, 2018, to assess whether she
13 had violated operational security by transmitting a list of NSW deployment records.

14 When Defendant was issued a computer for work, she signed a User Agreement
15 (ECF No. 92, Exh.1) in which she consented to the following conditions for her use of the
16 government computer:

- 17 (1) "The U.S. Government routinely intercepts and monitors
18 communications on this information system for purposes including, but
19 not limited to, . . . personnel misconduct, law enforcement, and
20 counterintelligence investigations."
- 21 (2) "At any time, the U.S. Government may inspect and seize data stored on
22 this information system."
- 23 (3) "Communications using, or data stored on, this information system are
24 not private, are subject to routine monitoring, interception and search and
25 may be disclosed or used for any U.S. Government authorized purpose."
- 26 (4) The security measures—such as the access card and PIN number for the
27 computer—are installed "to protect U.S. Government interests—not for
28 your personal benefit or privacy."

1 (5) Nonetheless, consent to this interception, monitoring, inspection and
2 seizing of data “does not negate any applicable privilege” such as
3 attorney-client, psychotherapist-patient or clergy-penitent. However,
4 users are strongly encouraged to seek personal legal counsel before using
5 the information system to communicate something the individual
6 believes to be privileged. And “[u]sers should take reasonable steps to
7 identify such communications or data that the user asserts are protected
8 by such privilege or confidentiality.”

7 (*Id.*)

8 To provide a reminder to the users of the conditions they agreed to in this User
9 Agreement, a warning banner appeared on all DoD computers when they were powered
10 up, essentially repeating all the conditions of consent that a user agreed to when using the
11 government-issued computer. (ECF No. 95, Exhs. 1 and 2.)

12 According to the Government, when the CISO reviewed Defendant’s military email
13 account, he discovered emails between Defendant and her husband that suggested she was
14 pricing military export-controlled items for sale to individuals in countries, such as the
15 PRC, without a license. Additionally, the CISO found communications that suggested
16 Defendant was using her position as a Logistics Supply Officer to obtain pricing
17 information for export-controlled items. Defendant communicated via email with Scott
18 Larson at Airborne Systems. His response included a warning that the information he was
19 providing was confidential and not to be disclosed. She promptly forwarded the email to
20 her husband.

21 Again, according to the Government, the CISO further found that Defendant used
22 her military email to request quotes for military equipment, changing her address at the last
23 minute from her SRT-I Command address to a personal address. The communications
24 resulted in companies shipping restricted products intended for U.S. military to recipients
25 that would normally have required additional verification.

26 Finally, NCIS located an Excel spreadsheet on the computer, in Mandarin, with
27 pages of lists of military devices and gear with associated website URL links and a resume
28 for her husband listing him as founder and manager of “5-Star Surplus.”

1 Discovery of these emails and documents on Defendant's military computer led to
2 search warrants and eventually to indictments against both Defendant and her husband.
3 (ECF No. 1.) Defendant's husband pled guilty to conspiracy to export defense articles
4 without a license and to export defense articles to an embargoed country and money
5 laundering. (ECF Nos. 47, 50.) Defendant faces charges for conspiracy to export defense
6 articles without a license, export defense articles to an embargoed country and commit theft
7 of government property, as well as exportation and attempted exportation of defense
8 articles without a license. (ECF No. 1.)

9 Defendant has filed this Motion to Suppress (ECF No. 92) arguing that all
10 information obtained from her military computer, including emails between her and her
11 husband, should be suppressed for violation of the Fourth Amendment. Defendant
12 maintains that anything seized as a result of any ensuing warrants based upon the
13 information in her computer should likewise be suppressed as fruit of the poisonous tree.

14 **II. ANALYSIS**

15 Defendant claims her employer—the Government—violated her Fourth
16 Amendment rights when it searched her computer. A defendant claiming her Fourth
17 Amendment rights were violated by a search must show that she has a "legitimate
18 expectation of privacy in the place searched or the item seized." *United States v. Zeigler*,
19 474 F.3d 1184, 1189 (9th Cir. 2007). This expectation is shown when the claimant
20 demonstrates both that she had a subjective expectation of privacy in the area searched and
21 that she had an objectively reasonable expectation of privacy in the area. *Id.* It is
22 defendant's burden to prove both of these elements. *Id.*

23 The Fourth Amendment clearly applies when the Government acts in its capacity as
24 an employer. *City of Ontario v. Quon*, 560 U.S. 746, 756 (2010); *see also O'Connor v.*
25 *Ortega*, 480 U.S. 709, 717 (1987) ("Individuals do not lose Fourth Amendment rights
26 merely because they work for the government instead of a private employer.").
27 Furthermore, computers can be particularly private spaces worthy of Fourth Amendment
28 protection. *See, e.g., Zeigler*, 474 F.3d at 1189.

1 However, public employees' expectations of privacy in their offices or computers
2 "may be reduced by virtue of actual office practices and procedures or by legitimate
3 regulation." *O'Connor*, 480 U.S. at 717. "[T]he validity of [any] expectation [of privacy]
4 depends entirely on its context." *Zeigler*, 474 F.3d at 1189.

5 Although use of a password on the computer can demonstrate a subjective
6 expectation of privacy, *id.*, in this case Defendant signed a User Agreement where she
7 specifically agreed that the security measures being taken—that is, an access card and PIN
8 number to access her computer—were installed to protect the Government's interests, not
9 for her own personal privacy, (ECF No. 92, Exh.1). She received a reminder specifically
10 reiterating this caution every time she used her computer. (ECF No. 95.) Thus, despite the
11 password protection, she could not have had a subjective expectation that the
12 communications from her computer were private.

13 Furthermore, Defendant received extensive warnings, both at the time her computer
14 was issued and her User Agreement was signed, as well as every time she opened her
15 computer and saw the banner admonishment, that the Government routinely monitored,
16 intercepted, inspected and seized communications made using her computer. She was
17 specifically told that the Government would be looking at her communications for evidence
18 of criminal wrongdoing, personnel misconduct and/or counterintelligence violations.
19 (ECF Nos. 92, Exh.1; 95.) As such, she also had no objectively reasonable expectation
20 that documents and emails on her computer would be private. *See United States v. Greiner*,
21 235 F. App'x 541, 542 (9th Cir. 2007) ("[P]rivacy expectations may be reduced if the user
22 is advised that information transmitted through the network is not confidential and that the
23 system administrators may monitor communications by the user." (quoting *United States*
24 *v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007))).

25 Defendant relies heavily on *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), to
26 support her argument that she still maintained an expectation of privacy in her computer
27 despite the banner warnings. However, the court in *Long* simply found that the lower court
28 was not clearly erroneous in determining that the defendant had a subjective expectation

1 of privacy in his military workplace computer emails. The court relied heavily on the
2 testimony of the network administrator who repeatedly said that the agency practice was
3 to recognize the privacy of employees' emails and that the banner described access that
4 would be completed to monitor the computer system and not to examine the contents of
5 the emails. Policies in place limited the network administrator's access to employees'
6 private emails. No such evidence has been presented in this case. *See United States v.*
7 *Larson*, 66 M.J. 212, 216 (C.A.A.F. 2008) (distinguishing *Long* for the same reasons).

8 Defendant argues that, despite the User Agreement and the banner warnings, she still
9 had an expectation of privacy in her emails to and from her husband because the User
10 Agreement specifically stated that an employee maintained all other applicable privileges.
11 Since she had a marital communication privilege with respect to her communications with
12 her husband, she argues, she reasonably expected that her employer would not look at these
13 communications.

14 As an initial matter, the Court takes notice of the fact that, although the Government
15 maintained that it would attempt to honor all other privileges, users needed to take
16 reasonable steps to identify privileged communications as such, so that the Government
17 would not unintentionally peruse privileged documents. Additionally, the Government
18 "strongly encouraged" users to seek personal legal counsel before using the government
19 computers to communicate any privileged material. Defendant took neither of these
20 precautions.

21 More importantly, however, in order for a marital communication to be privileged,
22 the party must have a reasonable expectation that the communications are confidential.
23 *United States v. Marashi*, 913 F.2d 724, 720 (9th Cir. 1990); *United States v. Hamilton*,
24 701 F.3d 404, 408–09 (4th Cir. 2012) (affirming determination of no marital privilege
25 when defendant took no steps to protect emails, even after he was on notice of employer's
26 policy permitting inspection of emails at employer's discretion). As discussed above,
27 given the vast array of warnings given to Defendant, she could not reasonably have
28 expected that any communications using her computer would be kept confidential.

1 Additionally, the marital communication privilege does not apply to
2 communications having to do with joint participation in a criminal endeavor. *Marashi*,
3 913 F.2d at 731. The communications seized from Defendant’s computer reflected her
4 communications with her husband planning the conspiracy with which she is now charged
5 and to which her husband has already pled guilty. Therefore, the communications were
6 not subject to the marital communications privilege. The fact that Defendant may have
7 thought they were privileged may go to her subjective expectation of privacy, but she still
8 fails to show that any expectation was objectively reasonable.

9 Furthermore, even if Defendant had a reasonable expectation of privacy in this
10 computer, the workplace exception laid out by the plurality in *O’Connor v. Ortega* applies.
11 In *O’Connor*, the Court held that any non-investigatory work-related intrusion by an
12 employer or an investigatory search for evidence of suspected work-related employee
13 misfeasance is inherently reasonable and not a violation of the Fourth Amendment. 480
14 U.S. at 721–722; *see also Quon*, 560 U.S. at 760 (noting the special needs of the workplace
15 is one area where a search warrant may not be required, as long as search is motivated by
16 a legitimate work-related purpose and was not excessive in scope); *United States v.*
17 *Slanina*, 283 F.3d 670, 679 (5th Cir. 2002) (“Under *O’Connor*, a search by a government
18 employer must be justified at its inception and reasonably related to the circumstances
19 justifying the interference in the first place.”), *vacated on other grounds*, 537 U.S. 802
20 (2002).

21 In this case, Defendant had a classified security clearance. An officer from SRT-I
22 expressed concern that Defendant was compiling a list of NSW Command deployment
23 personnel records. Thus, Defendant’s employer had a legitimate reason to conduct an
24 investigatory search for evidence of possible work-related misfeasance. The fact that the
25 misfeasance could potentially also be criminal conduct is of no import. *See Slanina*, 283
26 F.3d at 678 (“*O’Connor*’s goal of ensuring an efficient workplace should not be frustrated
27 simply because the same misconduct that violates a government employer’s policy also
28 happens to be illegal.”). Nor is it relevant that the government ultimately found no


1 evidence of misfeasance with respect to the compiling of personnel records but, instead,
2 found evidence of other criminal activity. The search that led to the discovery of the
3 criminal activity was reasonable under the *O'Connor* work place exception.

4 **III. CONCLUSION**

5 For the reasons stated above, Defendant's Motion to Suppress Evidence (ECF No.
6 92) is **DENIED**.

7 **IT IS SO ORDERED.**

8
9 **DATED: December 7, 2020**


Hon. Cynthia Bashant
United States District Judge